Creating an Entra ID Application for Veeam Backup for M365 Version 8 (needs to be tested in vcd first)

2025.04.22 20:49 AI-generated content may not always be authentic

how to create an entra ID application for Veeam Backup for M365 version 8, using modern authentication and including permissions for Exchange, Sharepoint, Onedrive, and Teams (backup and restore and all required permissions from any *.veeam.com documentation link).

Claude 3.7 Sonnet Think

Thought process ⌄

I'll need to search for the most current documentation on this topic, as Veeam Backup for Microsoft 365 v8 requires specific configurations for Entra ID (formerly Azure AD).

Searched 3 sites

- Step 5. Register or Select Microsoft Entra Application
- Adding Microsoft 365 Organizations with Modern App-Only ...
- Step 4. Configure Connection to Microsoft 365
- Permissions for Modern App-Only Authentication
- How to start with modern authentication in Veeam Backup
- Authentication Settings - Veeam Backup for Microsoft 365 ...
- Creating Applications - Veeam Backup for Microsoft 365 ...
- Veeam Backup for Microsoft 365: Installation and Configuration
- What You Do After Upgrade - Veeam Backup for Microsoft ...
- Configuring Veeam Backup for Microsoft Office 365 with ...

How to Create an Entra ID Application for Veeam Backup for M365 v8

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

Setting up an Entra ID application for Veeam Backup for Microsoft 365 version 8 with modern authentication requires configuring the proper permissions for Exchange, SharePoint, OneDrive, and Teams backup and restore. Based on the latest Veeam documentation, here's a comprehensive guide:

Option 1: Let Veeam Register the Application Automatically (Recommended)

When adding a Microsoft 365 organization to Veeam Backup for Microsoft 365, you can have Veeam register the application automatically:

- In the Veeam Backup for Microsoft 365 console, launch the **Add Organization** wizard
- Select your organization deployment type (including Teams if needed)
- At the **Configure Connection to Microsoft 365** step, select **Register a new Microsoft Entra ID application automatically** [ref:1,3]
- Provide the following:
  - In the **Name** field, enter a meaningful name for your new Entra ID application
  - Click **Install** to specify an SSL certificate for data exchange
  - You can either generate a new self-signed certificate or use an existing one
  - Select the **Grant the required permissions to this application and register its certificate in Microsoft Entra ID** checkbox [ref:1]
- When prompted, log in with a Microsoft 365 administrator account to grant the permissions

Option 2: Create and Configure the Application Manually

If you prefer to create the application manually:

- Log in to the Microsoft Entra ID admin portal (https://entra.microsoft.com)
- Navigate to **App registrations** and click **New registration**
- Enter a name for your application
- Select the appropriate supported account type (usually "Accounts in this organizational directory only")
- Click **Register**
- Note the **Application (client) ID** - you'll need this later

- Under **Certificates & secrets**:
  - Upload your certificate or generate a new client secret
  - If using a certificate, note the thumbprint
- Under **API permissions**, add the following permissions based on your backup requirements [ref:4]:

Required Permissions

Microsoft Graph API permissions:

- **Application permissions**:
  - `Directory.Read.All` – Reading directory data
  - `Group.Read.All` – Reading Microsoft 365 groups
  - `Group.ReadWrite.All` – Reading and restoring Microsoft 365 groups
  - `Mail.Read` – Reading users' mail
  - `Mail.ReadWrite` – Reading and restoring users' mail
  - `Sites.FullControl.All` – Reading and restoring SharePoint sites
  - `User.Read.All` – Reading users' profiles
  - `ChannelMessage.Read.All` – Reading channel messages
  - `Chat.Read.All` – Reading user chats
  - `TeamMember.Read.All` – Reading team members
  - `TeamMember.ReadWrite.All` – Reading and restoring team members
  - `ChannelMember.ReadWrite.All` – Reading and restoring Teams private and shared channels

Office 365 Exchange Online permissions:

- `EWS.AccessAsUser.All` – Accessing mailboxes through EWS

Office 365 SharePoint Online permissions:

- `Sites.FullControl.All` – Full control of site collections
- `User.Read.All` – Reading user profiles

- Click **Grant admin consent** for your organization

Adding the Application to Veeam Backup for Microsoft

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

365

After creating your Entra ID application manually, add it to Veeam:

- In the Veeam Backup for Microsoft 365 console, launch the **Add Organization** wizard
- At the **Configure Connection to Microsoft 365** step, select **Use an existing Microsoft Entra ID application** [ref:3]
- Provide the following:
  - **Application ID**: Enter the Application ID from your registered app
  - Click **Install** to specify the certificate you registered with the application
  - Select the certificate from the list or import it
  - You can check **Grant the required permissions to this application and register its certificate in Microsoft Entra ID** if you want Veeam to ensure all permissions are set [ref:1]

Special Considerations for Teams Backup

For Teams and Team Chats backup:

- You must use an existing Microsoft Entra ID application (you cannot register a new one automatically)
- Ensure the application has all the Teams-specific permissions listed above (`ChannelMessage.Read.All`, `Chat.Read.All`, etc.) [ref:3,4]

Global Reader Role for Public Folders & Discovery Mailboxes

For version 8, to back up public folder and discovery search mailboxes, and to correctly identify shared mailboxes:

- You need to grant the **Global Reader** role to your Microsoft Entra application after upgrading to version 8 [ref:4]

Certificate vs. Client Secret

- Veeam Backup for Microsoft 365 v8 supports both certificate-based and client secret authentication

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

- Certificate-based authentication is more secure and recommended for production environments
- When using a certificate, Veeam can register it in Microsoft Entra ID automatically

The application will now have all the required permissions to back up and restore Exchange, SharePoint, OneDrive, and Teams data from your Microsoft 365 organization with modern authentication.

how to create an entra ID application for Veeam Backup for M365 version 8, using modern authentication and including permissions for Exchange, Sharepoint, Onedrive, and Teams (backup and restore and all required permissions from any *.veeam.com documentation link).

o4-mini

Below is a step-by-step **manual** registration of an Entra ID (Azure AD) “daemon” app for Veeam Backup for Microsoft 365 v8, using certificate-based modern auth and granting **all** Exchange, SharePoint/OneDrive and Teams backup & restore permissions. You can find these details in Veeam’s official Help Center (any `*.veeam.com` link)—e.g.
• https://helpcenter.veeam.com/docs/vbo365/permissions.html?ver=80
• https://helpcenter.veeam.com/docs/vbo365/advanced-registration.html?ver=80

---

1. Register the App

- Sign in to the Entra ID portal:
  https://entra.microsoft.com → **Azure Active Directory** → **App registrations** → **New registration**
- Name: `VeeamBackupM365-v8` (or your convention)
- Supported account types: **Accounts in this organizational directory only**
- Redirect URI: leave blank (daemon app)
- Click **Register**.

Keep a note of the **Application (client) ID** and **Directory (tenant) ID**.

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

2. Configure Authentication

Certificate (recommended)

- In your app: **Certificates & secrets** → **Certificates** → **Upload certificate**
- Browse & upload a PEM/PFX-exported certificate (public key).
- Copy the **thumbprint**—you'll import this in Veeam.

> You may instead create a **Client secret** here, but cert-based auth is more secure.

---

3. Add API Permissions

In **API permissions** tab, click **Add a permission** → **Microsoft Graph** → **Application permissions**, then search & add:

• Directory.Read.All
• Group.Read.All
• Group.ReadWrite.All
• User.Read.All
• Mail.Read
• Mail.ReadWrite
• Sites.FullControl.All
• ChannelMessage.Read.All
• Chat.Read.All
• TeamMember.Read.All
• TeamMember.ReadWrite.All
• ChannelMember.ReadWrite.All

Next, **Add a permission** → **APIs my organization uses** → search **Office 365 Exchange Online** → **Application permissions** → add:

• EWS.AccessAsUser.All

> **Notes:**
> – `Sites.FullControl.All` covers both SharePoint and OneDrive data.
> – Teams chat backup/restore requires both `ChannelMessage.Read.All` and `Chat.Read.All`.

Finally, click **Grant admin consent for ⟨YourTenant⟩**.

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

4. (Optional) Assign “Global Reader” Role

Veeam v8 requires **Global Reader** on your tenant to discover Public Folders & Discovery Mailboxes:

- Entra ID → **Roles and administrators** → **Global Reader** → **Add assignments**
- Select your registered app → **Add**.

---

5. Configure Veeam Backup for Microsoft 365

- Open Veeam Backup for Microsoft 365 console → **Add Organization**
- At **Connection to Microsoft 365** choose **Use existing Microsoft Entra ID application**
- Enter:
  - **Application ID**: (from step 1)
  - **Tenant ID**: (from step 1)
  - **Certificate thumbprint** (or client secret if used) → click **Install**
- Check **Grant the required permissions…** if you want Veeam to verify/consent automatically
- Finish the wizard.

Veeam will now use modern (OAuth 2.0) authentication with your app’s cert, and has all rights to back up and restore Exchange mailboxes, SharePoint sites/OneDrives, Teams (channels & chat).

how to create an entra ID application for Veeam Backup for M365 version 8, using modern authentication and including permissions for Exchange, Sharepoint, Onedrive, and Teams (backup and restore and all required permissions from any *.veeam.com documentation link). assume the user has never used portal.azure.com so be very specific

GPT-4.1

Thought process ⌄

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

Certainly! Here is a **very specific, step-by-step guide** to manually create an Entra ID (Azure Active Directory) application for **Veeam Backup for Microsoft 365 v8** using modern authentication, including backup & restore permissions for Exchange, SharePoint, OneDrive, and Teams. All permissions and process steps are referenced from official Veeam documentation:

- Veeam: Required Permissions
- Veeam: Registering Your Own Azure AD Application

Step 1: Log in to the Entra ID (Azure AD) Portal

- Open your web browser and go to: https://entra.microsoft.com
  (If that does not work, use https://portal.azure.com, then search for "Microsoft Entra ID.")
- **Sign in** with your Microsoft 365 administrator account.

Step 2: Register a New Application

- In the portal, on the left menu, click "**Home**" if not already there.
- Click "**Microsoft Entra ID**" (may also be "Azure Active Directory").
- In the left menu, click "**App registrations**".
- At the top, click "**New registration**".

In the registration form:

- **Name:** Enter something recognizable, e.g. `VeeamBackupM365`
- **Supported account types:** Choose the first option: "**Accounts in this organizational directory only...**"
- **Redirect URI:** Leave empty (not needed).

- Click "**Register**" at the bottom.

Step 3: Note Down Important Details

Once the app is registered, you'll be taken to its "Overview" page:

- **Copy and save these:**
  - **Application (client) ID**
  - **Directory (tenant) ID**

You'll need these for Veeam later.

Step 4: Add a Certificate for Authentication

This is required for modern, secure authentication.

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

A. Generate a Certificate

If you don’t have a certificate, you can create one using PowerShell (on your PC):

```powershell
New-SelfSignedCertificate -CertStoreLocation "cert:\CurrentUser\My" -Subject "CN=VeeamBacku
```

- Find it in Windows "**Manage user certificates**" under "**Personal > Certificates**".
- **Export certificate:**
  - Right-click the certificate → **All Tasks > Export**
  - Choose "No, do not export the private key"
  - Save as **.CER file** (public key).

B. Upload Certificate to Entra ID

- In the Azure portal, go to your app’s **Certificates & secrets** (left menu).
- Under **Certificates**, click "**Upload certificate**"
- Select the **.CER** file you just exported.
- Click **Add**.

Step 5: Add API Permissions

This step is critical! All permissions must be **Application** type.

- In your app’s menu, click "**API permissions**".
- Click "**Add a permission**".
- Click "**Microsoft Graph**" → "**Application permissions**".
  - In the search box, add these (one at a time, type the text and tick the box):
    - `Directory.Read.All`
    - `Group.Read.All`
    - `Group.ReadWrite.All`
    - `Mail.Read`
    - `Mail.ReadWrite`

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

    - `Sites.FullControl.All`
    - `User.Read.All`
    - `ChannelMessage.Read.All`
    - `Chat.Read.All`
    - `TeamMember.Read.All`
    - `TeamMember.ReadWrite.All`
    - `ChannelMember.ReadWrite.All`

- **Still under "Add a permission,"** click **"APIs my organization uses"**, search for **"Office 365 Exchange Online"**.
    - Select "**Application permissions**".
    - Tick **`EWS.AccessAsUser.All`**

- Click **"Add permissions"** when done for each API.

- In the "API permissions" list, click **"Grant admin consent for [YourTenant]"**.
    - Confirm in the popup.

More permission info: Veeam Required Permissions Table

Step 6: Assign the "Global Reader" Role (Required for Public Folders/Discovery Mailboxes)

- In Entra ID (left menu), click **"Roles and administrators"**.
- Find **"Global Reader"** and click it.
- Click **"Add assignments"** at the top.
- Select your newly registered app.
- Click **"Add"**.

Step 7: Set Up in Veeam Backup for Microsoft 365

- Open the Veeam Backup for Microsoft 365 Console.
- Go to **"Organizations"** → Click **"Add Organization"**.

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

- When prompted for Microsoft 365 authentication, select "**Use an existing Microsoft Entra ID application**".
- Enter:
  - **Application (client) ID** (from Step 3)
  - **Directory (tenant) ID** (from Step 3)
  - Import the **certificate** file (the same `.CER` you used earlier)
- Complete the setup wizard.

If you get a permissions error, double-check that all the permissions were granted and "admin consent" was given in Step 5.

Summary Table of Required Permissions

Refer to Veeam's own chart:
https://helpcenter.veeam.com/docs/vbo365/permissions.html?ver=80

Table

Platform	Permission Name	Type
Microsoft Graph	Directory.Read.All	Application
Microsoft Graph	Group.Read.All / ReadWrite.All	Application
Microsoft Graph	Mail.Read / ReadWrite	Application
Microsoft Graph	Sites.FullControl.All	Application
Microsoft Graph	User.Read.All	Application
Microsoft Graph	ChannelMessage.Read.All	Application
Microsoft Graph	Chat.Read.All	Application
Microsoft Graph	TeamMember.Read.All / ReadWrite.All	Application
Microsoft Graph	ChannelMember.ReadWrite.All	Application
Exchange Online	EWS.AccessAsUser.All	Application

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF

Documentation Quick Links:

- Register your own Azure AD application
- Required Permissions Table

Let me know if you'd like screenshots or more about using the Veeam console!

Explore our developer-friendly HTML to PDF API Printed using PDFCrowd HTML to PDF